Chapter 1

Computer Security: protection afforded to information system in order to attain
- integrity
- availability
- confidentiality

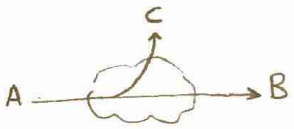
Example of Security Requirements
- integrity : No body can change it ; Patient information
- availability: authentication service
- confidentiality : No body can see it , student grades

Network Security : Protection the transportation of data → send and ← receive

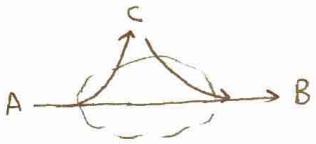
Aspects of security
1. attack
2. mechanism
3. services

Attack

Passive attack :
- do not change any thing
- more dangerous than active
- Ex. - monitoring network
  - copy msg.



Active attack :
- do change
- Ex. - modify msg.
  - replay msg.
  - DoS : Dinal of service
  - masquerade (Pretend)



Security services : enhance security of data processing system and information transfers of an organization

Authentication: assurance that communication entity is the one claimed

Access Control: prevention of the unauthorized use of a resource

Data confidentiality : protection of data from unauthorized disclosure.

Non-Repudiation: protection against denial by one of the Parties in Communicatio

Data integrity : assurance that the data received as sent by authorized entity

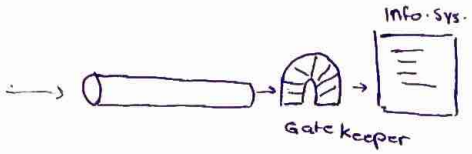
Availability : resource accessible / usable

Security Mechanism : feature designed to detect, prevent or recover from a security attack.

- there is no single mechanism that will support all services required

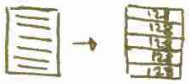
Model of Network Security

Model for Network Access Security



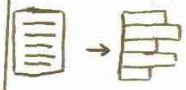
Chapter 3 : Data Encryption Standard (DES)

Block Ciphers



- process messages in blocks
- Ex. Substitution on very big character
- many current ciphers are block ciphers?
  - better analysed
  - broader range of App.
- Symmetric block cipher based on Feistel Cipher structure.
- look like an extremely large substitution

Stream Ciphers



- process messages a bit or byte

What is the two type of cryptographic operations?

- Substitution : man → MaN
- transposition : man → nam

Confusion

- makes relationship between chiphertext and key as complex as possible.
- $C \overset{\text{cipher}}{\longleftrightarrow} K$
- Substitution lead to Confusion

Diffusion

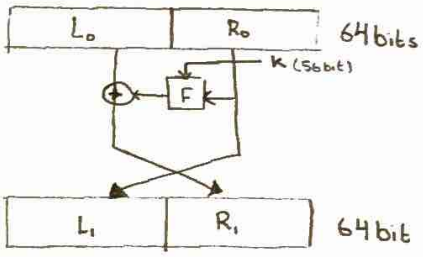
- Small change in plaintext effect all chiphertext
- P : mon → C : A x y
- P : man → C : N H F

only letter o change in plaintext but all letter change in ciphertext

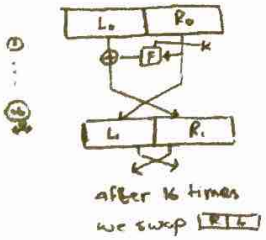
---

Feistel Cipher : input block into two halves

- we do swaping 16 times
- in each round we have
  - 2 transposition
  - 1 substitution
- in each round we increase Confusion and diffusion
- every round requerd diffrent Subkey



DES Encryption



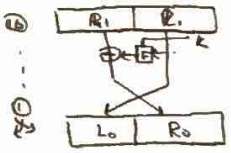
$L_1 = R_0$

$R_1 = L_0 \oplus F(R_0, K)$

$C = L_1 \| R_1$

DES Decryption

we do encryption again using subkeys in reverse order



$L_0 = L_1 = R_0$

$R_0 = R_1 \oplus F(L_1, k)$

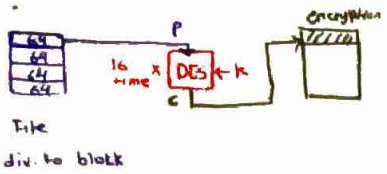
$= L_0 \oplus F(R_0, k) \oplus F(\overset{R_0}{L_1}, k)$ 1 XOR 1 = 0

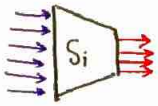
$= L_0 \oplus 0$

$= L_0$

$C = L_0 \| R_0$

DES Round Structures





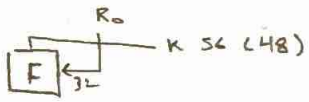
input 6 → S-box → 4
non-linear (mush difficult) complex to gain confusion
- we use fix table for S-box and diffren key

Avalanche

- A change of one input or key bit results in changing approx half out put bits
- 50% Avalanche → good Diffusion
- $\frac{64 \text{ bits}}{2}$ = 32 bit diffrent to have avalanche
- Why we do 16 round in DES?
  because we need to have avalanche
  16 × 2 = 32
  at round at least 2 change
  (change) effects

How good is the algorithm?

Encrypt 64 bit Using 56 bit key
↓
small key
we need larger



Plain text = 48
key = 56
sub key ① ... ⑯
48 48

- weakness the key size

* 32 : 32 because hardware

* DES implemente in software and hardware
  slow faster
  only update but we should
  bluid it

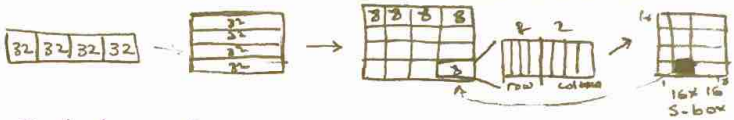
* we focuse in speed if the algorithm is slow even when it secure we don't want it

Chapter 5: Advanced Encryption Standard (AES)

- it's take 3 to 4 years to select AES
- * AES has 128 / 192 / 256 bit keys, has 10 / 12 / 14 → 9 / 11 / 13 round (final round has only 3 stages)
- * AES an iterative cipher rater than feistel.
  - iterative: work withall data + less time
  - feistel: work with half data + more time
- * AES designed to be:
  - resistant against known attack
  - speed and code compactness on many CPUs
  - design simplicity

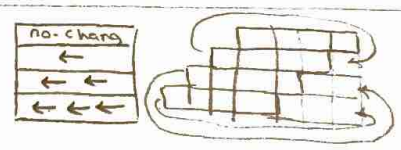
AES

1. Substitution Bytes



- each byte of state is replaced by byte
- this step lead to confusion

2. Shift Rows



- For encryption: shift to left ←
- For decryption: shift to right →
- this step lead to diffusion.

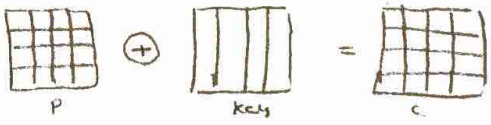
3. Mix Columns

$$\begin{bmatrix} & \end{bmatrix} \times \begin{bmatrix} & \end{bmatrix} = \begin{bmatrix} & \end{bmatrix}$$

change in one value effect 4 value

- encryption = $M \times S = C$
- decryption = $M^{-1} \times C = S$

4. Add Round key



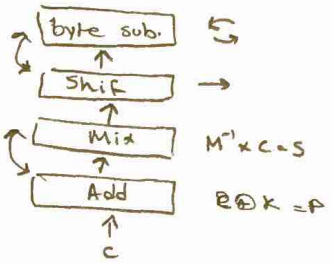
- the only step that use the key

AES Avalanche

- Avalanche is done on Mix column + Shift Rows
- $\frac{128 \text{ bit}}{2} = 64$

AES Decryption

- do the reverce of each step 10 time.
- result unchange when
  - swap byte substitution and shift row
  - swap mix column and add round key.



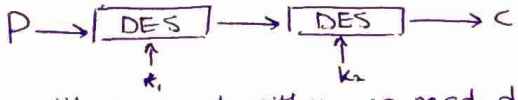
P
↓
Add
Byte
Shif
Mix
Add
↓
C

C
↓
Add
Byte
Shif
Mix
Add
↓
P

* we always start with Add round key because it's the one that have key
* we do other step for complexity & security

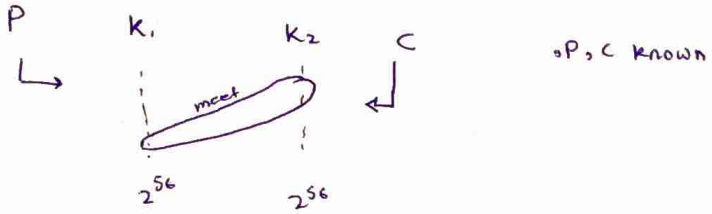
Chapter 6 : Block Cipher Operation

Double - DES



- with new algorithm we need double time to break it

Problem:



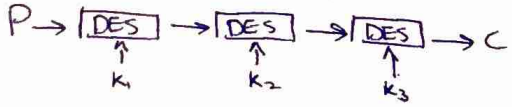
• P, C known

∴ the problem is meet-in-the-middle.

Solve :

Triple - DES

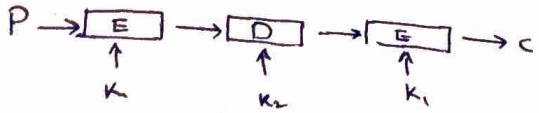
- Using 3-keys



$k_1 + k_2 + k_3 = 56 + 56 + 56 = 168$

$\frac{2^{168}}{2} = 2^{167}$

- Using 2-keys

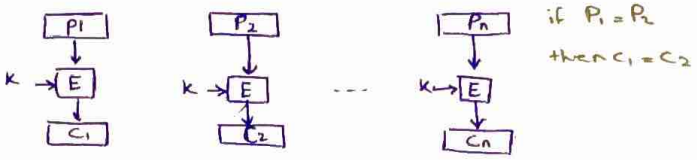
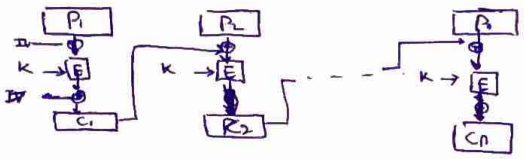
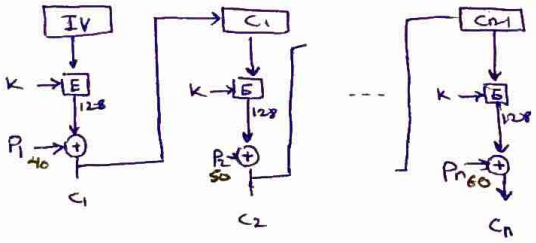
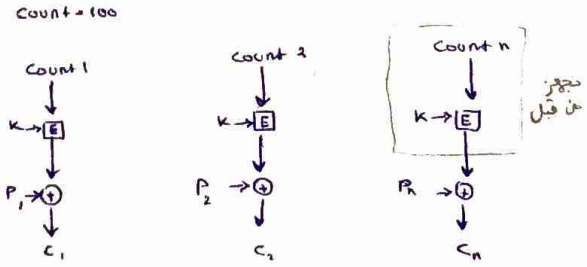


- can work with single DES

-ve:

- Slow
- Small blocks

Modes of Operation

modes Name	decr.	Advantages and Limitations
Electronic Code book Book (ECB)	 if $P_1 = P_2$ then $C_1 = C_2$ - message is broken into independent block which are encrypted - Uses: secure transmission of single value	+ve: - encoded independently of other block - simple -ve: - message repetitions may show in ciphertext
Cipher Block Chaining (CBC)	 - message is broken into block - linked together in encryption - each previous chipher blocks is chaind with current Plaintext. - Uses: bulk data encryption, authentication.	+ve: No repetitions -ve: - no parallel processing - error in one may effcte other - need IV
Cipher FeedBack (CFB)		+ve: - we can work with stream - No need for decryption algorithm -ve: - no parallel processing - error in one effct the other.
Counter (CTR)	 - must have different key & counter value for every Plaintext - Uses: high-speed network encryption	+ve: - can do parallel pro - no chain - faster -ve: - we should chang counter - never reuse same counter